REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

I. STATUTORY DOUBLE PATENTING

The Examiner submits that claims 7 and 9 of the present Application conflict with claims 1 and 3 of co-pending, commonly assigned U.S. Patent Application Serial No. 09/944,788 (hereinafter "the '788 Application"). The Examiner requests that the allegedly conflicting claims be cancelled from either the present application or from the '788 Application, in accordance with 37 CFR §1.78(b). The Applicants respectfully submit, however, that the requested cancellation of claims is inappropriate.

In particular, the Applicants submit that claims 7 and 9 of the present Application do not conflict with claims 1 and 3 of the '788 Application under the meaning of 37 CFR §1.78(b). The Examiner indicated as much in the Final Office Action by stating that "[t]he claims of the current application are broader than the claims of the 09/944,788 application" (page 2, emphasis added). Thus, claims 7 and 9 of the present Application and claims 1 and 3 of the '788 Application are not coextensive in scope. MPEP 804.02. Accordingly, the Applicants respectfully request that the statutory double patenting rejection of claims 7 and 9 be withdrawn.

II. REJECTION OF CLAIMS 1-2 AND 4-9 UNDER 35 U.S.C. § 102

1. Claims 1, 2, 4 and 5

Claims 1, 2, 4 and 5 stand rejected as being anticipated by the Baker patent (U.S. 6,775,657, issued November 19, 2002, hereinafter "Baker"). The Applicants respectfully traverse with the rejection.

Particularly, the Examiner's attention is directed to the fact that Baker fails to disclose or suggest the novel invention of transmitting information about a second sensor's belief state to a first sensor in an intrusion detection system, where the belief state indicates a state of a system resource or service and adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed

in Applicants' independent claims 1, 4 and 5.

Baker does not teach, show or suggest sensors that maintain a belief state indicating a state of a system resource or service. Even if it were assumed that the sensors described by Baker could be considered to maintain "belief states", Baker does not teach, show or suggest that a given sensor's belief state may be modified based on the belief state of another sensor. In fact, nowhere does Baker teach or suggest that a sensor can communicate or share information with other sensors at all. Baker at most teaches that sensor data may be transmitted to one or more directors (*See, e.g.*, Baker at column 7, lines 35-41 and column 8, lines 17-22). Thus, Baker does not teach that a first sensor can transmit a belief state to a second sensor, or that the second sensor can modify its own belief state based on the belief state received from the first sensor.

Notably, Applicants' invention claims a method in which a first sensor's belief state regarding a state of a network resource or service is adjusted based on at least part of a second sensor's belief state, as recited by the Applicants in independent claims 1, 4 and 5. Specifically, Applicants' claims 1, 4 and 5 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service; and

(b) adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service, the adjustment based at least in part on the second sensor's belief state. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a monitored resource; and

(b) adjusting a prior belief state of the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm. (Emphasis added)

5. A method for enhancing the sensitivity of an intrusion detection system that

monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on monitored computer system resources; and

(b) adjusting a prior belief state of the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious. (Emphasis added)

As discussed above, nowhere does Baker teach or even suggest the desirability of adjusting a belief state of a sensor relating to a state of a monitored system resource or service supported thereon, based on a belief state of another sensor. Therefore, the Applicants submit that independent claims 1, 4 and 5 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not anticipated by the teachings of Baker. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

2. Claims 6-9

Claims 6-9 stand rejected as being anticipated by the Bristol patent (U.S. 6,690,274, issued February 10, 2004, hereinafter "Bristol"). The Applicants respectfully traverse the rejection.

Particularly, the Examiner's attention is directed to the fact that Bristol fails to disclose or suggest the novel invention of organizing alerts into classes by evaluating a similarity between a new alert and an existing class of alerts, including adjusting or updating an expectation that feature values of the new alert and feature values of the existing alert class will match, as claimed in Applicants' independent claims 6, 7 and 9.

Firstly, Bristol fails to teach or even suggest the desirability of or adjusting or updating an expectation that feature values of a new alert and feature values of an existing alert class will match. As described in the Applicants' specification, the nature of an alert may affect a similarity expectation that indicates which features (*e.g.*, source

IP address, destination IP address, type of attack, etc.) of the alert should be similar to corresponding features of an existing alert class (*See*, for example, page 6, lines 15-18 and page 7, line 13 – page 9, line 11). For example, if a new alert indicates a SYN flood attack (in which source IP addresses are typically forged), similarity of source IP addresses might not provide a meaningful basis for comparison between the new alert and an existing alert class. Thus, when comparing the new alert to an existing alert class for correlation purposes, it may be necessary to adjust or update this similarity expectation in order to make a meaningful comparison.

The portion of Bristol that the Examiner cites as allegedly teaching this limitation at most teaches that a group of generated alarms is scanned for alarms that match user-selected criteria (*e.g.*, certain full or partial character patterns). Bristol does not teach, however, that analysis of a given alarm based on the user-selected criteria is adjusted or updated by an expectation that features values the given alarm and the user-defined criteria will match.

Secondly, Bristol does not teach defining a new alert class if a newly generated alert does not correspond to an existing alert class. This limitation is completely overlooked by the Examiner's analysis of claims 6-9 in the Final Office Action. Bristol is directed not to a method that seeks to classify each generated alarm, but rather to a method that scans generated alarms for those that exemplify specific desired criteria. Thus, if a given alarm does not exemplify the desired criteria for which the method is scanning, there is no need to treat the given alarm any further.

Notably, Applicants' invention claims a method in which alerts are grouped into classes based on similar feature values, an expectation that feature values of a new alert and feature values of an existing alert class will match is adjusted or updated, and a new alert class is defined if the new alert does not match an existing alert class, as recited by the Applicants in claims 6, 7 and 9. Specifically, Applicants' claims 6, 7 and 9 positively recite:

6. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) identifying a set of potentially similar features shared by a new alert and one or more existing alert classes;

(b) comparing the new alert to one or more existing alert classes;
(c) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
(d1) associating the new alert with the existing alert class that the new alert most closely matches; or
(d2) defining a new alert class that is associated with the new alert. (Emphasis added)

7. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:
(a) receiving a new alert;
(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
(c) updating a similarity expectation for one or more feature values;
(d) comparing the new alert with one or more alert classes, and either:
(e1) associating the new alert with the existing alert class that the new alert most closely matches; or
(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

9. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:
(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding features;
(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
(c) comparing the new alert to one or more alert classes;
(d) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
(e1) associating the new alert with the existing alert class that the new alert most closely matches; or
(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

As discussed above, nowhere does Bristol teach or even suggest the desirability of adjusting or updating an expectation that feature values of a new alert and feature values of an existing alert class will match is adjusted or updated or defining a new alert class if the new alert does not match an existing alert class. Therefore, the Applicants submit that independent claims 6, 7 and 9 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 8 depends from claim 7 and recites additional features

therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 8 is not anticipated by the teachings of Bristol. Therefore, the Applicants submit that dependent claim 8 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

III. REJECTION OF CLAIM 3 UNDER 35 U.S.C. § 103

Claim 3 stands rejected as being unpatentable over Baker in view of the Timm patent (U.S. 5,440,498, hereinafter "Timm"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Baker and Timm, singularly or in any permissible combination, fail to disclose or suggest the novel invention of transmitting information about a second sensor's belief state to a first sensor in an intrusion detection system, where the belief state indicates a state of a system resource or service and adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed in Applicants' independent claim 1, from which claim 3 depends. Applicants' claim 1 has been recited above.

As discussed above, nowhere does Baker teach or even suggest the desirability of adjusting a belief state of a sensor relating to a state of a monitored system resource or service supported thereon, based on a belief state of another sensor. Timm does not bridge this gap in the teachings of Baker. Baker and Timm, singularly or in any permissible combination, thus fail to teach, suggest or make obvious a method in which a first sensor's belief state relating to a state of a network resource or service is adjusted based on at least part of a second sensor's belief state, as positively claimed by the Applicants in claim 1. Therefore, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claim 3 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 3 is not made obvious by the teachings of Baker in view of Timm. Therefore, the Applicants submit that dependent claim 3 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

IV. INFORMATION DISCLOSURE STATEMENT

The Applicants will shortly be filing an Information Disclosure Statement in connection with the present Application. The Examiner is respectfully encouraged to review the references that the Applicants will be providing in connection with any response to this communication.

V. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

2/24/06
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702